

This international application for which the EPO is a designated office has not been republished by the EPO according to article 158(1) EPC.

ERTU DU TRAITÉ DE COOPÉRATION
ETS (PCT)

Intellectuelle
Bureau international



(43) Date de la publication internationale
4 juillet 2002 (04.07.2002)

PCT

(10) Numéro de publication internationale
WO 02/052515 A1

(51) Classification internationale des brevets⁷ : G07F 7/10

(21) Numéro de la demande internationale :
PCT/IB01/02603

(22) Date de dépôt international :
19 décembre 2001 (19.12.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2000 2519/00 22 décembre 2000 (22.12.2000) CH

(71) Déposant (pour tous les États désignés sauf US) :
NAGRAVISION SA [CH/CH]; Route de Genève 22,
CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : JAQUIER,
Jean-Luc [CH/CH]; Route de Corsy 35, CH-1093 La Con-
version (CH). SASSELLI, Marco [CH/CH]; Chemin des
Roches 20, CH-1803 Chardonne (CH).

(74) Mandataire : LEMAN CONSULTING SA; Route de
Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,
ZW.

19.12.01

+24 19.12.03 +6 +17 6.06

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR,
IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ,
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,
TD, TG).

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: MATCH CONTROL METHOD

(54) Titre : MÉTHODE DE CONTRÔLE D'APPARIEMENT

(57) Abstract: The invention aims at providing a method which guarantees encryption of data exchanged between a security module and a user unit through a matching key specific to the user unit/security module pair, while allowing the possibility to the security module to be matched with other units. Therefor, the invention provides a method which consists in: detection by the user unit whether the connected security module is matched therewith; if that is so, using a unique key specific to the user unit/security module pair to encrypt the exchanged data; otherwise, requesting from the management centre authorisation to be matched with said security module, the request being accompanied by identifiers of the user unit and of the security module; verification by the management centre the conformity of said matching and transmission of the result to the user unit; if authorisation is granted, establishing a unique key specific to the user unit/security module pair to encrypt the exchanged data.

(57) Abrégé : Le but de la présente invention est de proposer une méthode qui garantit l'encryptage des données échangées un module de sécurité et une unité d'utilisateur par une clé d'appariement propre au couple unité d'utilisateur / module de sécurité, en toutefois laissant la possibilité au module de sécurité d'être apparié avec d'autres unités d'utilisateur. Selon l'invention, ce but est atteint par une méthode consistant à :- détecter par l'unité d'utilisateur si le module de sécurité connecté lui est apparié, - dans l'affirmative, utiliser une clé unique propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées, - dans la négative, requérir auprès du centre de gestion l'autorisation de s'apparier avec ce module de sécurité, requête accompagnée des identifiants de l'unité d'utilisateur et du module de sécurité, - vérifier par le centre de gestion la conformité de cet appariement et transmettre le résultat à l'unité de l'utilisateur, - si l'autorisation est donnée, établir une clé unique propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées.

WO 02/052515 A1

BEST AVAILABLE COPY

METHODE DE CONTROLE D'APPARIEMENT

La présente invention concerne une méthode de contrôle de transfert sécurisé d'informations entre une unité d'utilisateur et un module de sécurité, en particulier lors de l'interaction de ce module de sécurité avec
5 plusieurs unités d'utilisateurs.

Ces unités d'utilisateur sont connectées à un ou des réseaux proposant des produits ou services.

Ces produits ou services étant à accès conditionnel, l'utilisation de ces produits est soumise à un paiement sous forme quelconque, par exemple
10 par abonnement ou achat spécifique.

Ces unités d'utilisateur se présentent sous plusieurs formes, par exemple un décodeur de télévision à péage, un ordinateur voire un téléphone portable, un "palm-top", un PDA, une radio, une télévision une borne multimédia, un distributeur de billet.

15 Par produit ou service, on entend non seulement un film, une retransmission sportive, de la musique, un programme informatique, un jeu, des informations boursières ou des actualités mais également un service tel que l'accès et l'utilisation d'un réseau, l'identification ou le paiement électronique. Ce produit ou services est accessible sur un
20 réseau sur lequel les utilisateurs peuvent se connecter et utilise des moyens d'encryptage pour l'aspect sécurité.

Pour gérer les autorisations d'utilisation de ces produits ou services, l'unité d'utilisateur comprend des moyens de sécurité placés dans un module de sécurité.

Ce module de sécurité se présente généralement sous la forme d'une carte à puce, de la forme d'une carte de crédit ou d'une puce, voire d'une SIM, comprenant un crypto-processeur (USIM, WIM). Cette carte permet de fournir les informations nécessaires pour autoriser l'utilisation du produit par l'intermédiaire des opérations de décryptage utilisant des clés stockées dans la mémoire du crypto-processeur réputée inviolable.

Ce module de sécurité est amené à échanger des informations confidentielles avec l'unité d'utilisateur, par exemple lorsqu'il s'agit de transmettre la clé de décryptage du produit dans le cadre de la télévision à péage, cette clé étant décryptée dans le module de sécurité et transmise à l'unité d'utilisateur pour traiter les données.

C'est pourquoi, pour empêcher toutes atteintes à ces données, la voie de communication entre le module de sécurité et l'unité d'utilisateur est encryptée par une clé unique à ces deux éléments dite clé d'appariement. Cette configuration est décrite dans la demande PCT/IB99/00821 dans laquelle la clé unique est initialement dans le décodeur et est ensuite chargée dans le module de sécurité lors d'une phase d'initialisation. Une fois le module de sécurité apparié avec le décodeur, ce module ne peut fonctionner dans aucune autre unité.

Cette solution présente le premier inconvénient d'empêcher toute utilisation du module de sécurité dans un autre décodeur, même si ce décodeur appartient au même utilisateur. Un autre inconvénient de cette méthode est qu'elle n'empêche pas l'utilisation d'une carte clonée qui serait utilisée pour la première fois dans un décodeur quelconque et donc appariée avec ce décodeur.

Le but de la présente invention est de proposer une méthode qui garantit l'encryptage des données échangées entre le module de sécurité et l'unité d'utilisateur tout en palliant aux inconvénients cités ci-dessus.

Ce but est atteint par une méthode d'appariement entre un module de sécurité et une unité d'utilisateur, cette dernière disposant de moyens de communication bidirectionnels avec un centre de gestion, caractérisée en ce qu'elle consiste à :

- détecter par l'unité d'utilisateur si le module de sécurité connecté lui est apparié,
- 10 - dans l'affirmative, utiliser une clé unique d'appariement propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées,
- dans la négative, requérir auprès du centre de gestion l'autorisation de s'apparier avec ce module de sécurité, requête accompagnée des
15 identifiants de l'unité d'utilisateur et du module de sécurité,
- vérifier par le centre de gestion la conformité de cet appariement et transmettre le résultat à l'unité de l'utilisateur,
- si l'autorisation est donnée, établir une clé d'appariement propre au couple unité d'utilisateur / module de sécurité pour encrypter les données
20 échangées.

Ainsi, le contrôle de l'appariement est effectué de manière dynamique et n'est plus la conséquence de la connexion d'un module de sécurité dans une unité d'utilisateur. Il est géré par le centre de gestion qui décide d'accepter ou de refuser cet appariement. C'est pourquoi la requête est
25 accompagnée des données permettant d'identifier ces deux éléments tels que leurs numéros de série par exemple. Il peut être accompagné de

données concernant la localisation de l'unité, données obtenues par d'autres voies, par exemple le numéro d'appel de l'unité ou l'adresse sur son réseau.

5 Par clé d'appariement, on entend une clé symétrique ou une clé asymétrique, par exemple une clé publique et une clé privée. Dans ce dernier cas, les trois cas suivants peuvent se présenter:

- chaque partie comprend les deux clés publiques et privées. Les communications vers l'autre partie sont encryptées par la clé publique et donc décryptées par la clé privée.
- 10 - chaque partie contient l'une des clés publique ou privée. Dans une direction, les données seront encryptées par la clé publique puis décryptées par la clé privée, et dans l'autre direction les données sont encryptées par la clé privée puis décryptées par la clé publique.
- chaque partie contient la clé publique de l'autre partie et sa clé privée.
- 15 Les données sont encryptées par la clé publique de l'autre partie et décryptées par sa propre clé privée.

Il est à noter qu'un module de sécurité peut être apparié avec plusieurs unités d'utilisateur. Sa mémoire dispose d'une zone pour stocker un ensemble de clés d'appariement, chaque clé étant associée au numéro d'identification de l'unité d'utilisateur.

20

Ainsi, lors de chaque connexion d'un tel module dans une unité d'utilisateur, le protocole d'initialisation inclut la reconnaissance mutuelle et l'utilisation de la clé (ou des clés) propre au couple unité d'utilisateur / module de sécurité.

Selon une variante de l'invention, l'unité d'utilisateur peut également disposer d'une zone de clés d'appariement et peut être de ce fait appariée avec plusieurs modules de sécurité.

5 Cette clé unique peut être générée de plusieurs manières. Elle peut être générée par le centre de gestion et transmise avec l'autorisation d'appariement, bien entendu sous forme encryptée. Cette clé est transmise au module de sécurité en utilisant une encryption établie selon une clé de session selon des procédures connues en soi.

10 Un autre moyen d'obtenir cette clé propre est de la générer soit dans l'unité d'utilisateur, soit dans le module de sécurité, soit partiellement dans l'un et l'autre de ces éléments, la combinaison formant alors la clé.

15 Dans une forme de réalisation de la méthode de l'invention, la requête au centre de gestion est accompagnée non seulement des données identifiants le couple unité d'utilisateur / module de sécurité mais également accompagnée par les données comprises dans la zone de mémoire d'appariement c'est-à-dire incluant tous les appariements précédents.

20 Le centre de gestion peut alors vérifier que ce module de sécurité a bien été apparié aux unités d'utilisateur qu'il a autorisé, et selon l'ordre des requêtes.

Ainsi, si un module de sécurité a été cloné, lorsque ce module cloné va demander à s'apparier avec une unité d'utilisateur, les données transmises au centre de gestion concernant les précédents appariements seront différentes de celles du module d'origine. Le centre de gestion dispose de
25 ce fait de moyens pour identifier les modules clonés.

Dans un premier temps, le centre de gestion va accepter l'appariement de cette carte clonée avec une nouvelle unité d'utilisateur B. Si le clonage d'une carte authentique a été opérée à large échelle, la prochaine carte clonée, ayant le même identifiant, requérant l'appariement avec une nouvelle unité d'utilisateur C, le centre de gestion ne retrouvera pas de trace du précédent appariement avec l'unité d'utilisateur B. Cette indication permettra de détecter une tentative de fraude et réagir en conséquence. De plus, si l'utilisateur de la carte authentique désire l'utiliser avec une nouvelle unité D, les données d'appariement transmises par ce module ne contiendront aucune trace de l'unité C et le centre de gestion refusera l'appariement, voire provoquera le blocage complet de ce module de sécurité.

REVENDEICATIONS

1. Méthode de contrôle d'appariement entre un module de sécurité et une unité d'utilisateur, cette dernière disposant de moyens de communication bidirectionnels avec un centre de gestion, caractérisée en ce qu'elle consiste à :

- détecter par l'unité d'utilisateur si le module de sécurité connecté lui est apparié,
- dans l'affirmative, utiliser une clé d'appariement propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées,
- dans la négative, requérir auprès du centre de gestion l'autorisation de s'apparier avec ce module de sécurité, requête accompagnée des identifiants de l'unité d'utilisateur et du module de sécurité,
- vérifier par le centre de gestion la conformité de cet appariement et transmettre le résultat à l'unité de l'utilisateur,
- si l'autorisation est donnée, établir une clé d'appariement propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées.

2. Méthode selon la revendication 1, caractérisée en ce que la clé d'appariement est soit une clé symétrique, soit une clé asymétrique, soit une paire de clés asymétriques.

3. Méthode selon la revendication 1 ou 2, caractérisée en ce qu'elle consiste à stocker dans le module de sécurité, la clé d'appariement avec l'identifiant de l'unité d'utilisateur propre à cette unité.

4. Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle consiste à transmettre les données des appariements précédents au centre de

gestion, ce dernier vérifie ces données avec l'image des appariements autorisés associés à l'identifiant de ce module de sécurité.

5. Méthode selon les revendications 1 à 4, caractérisée en ce que la clé d'appariement est générée dans le centre de gestion et est transmise à l'unité d'utilisateur et au module de sécurité sous forme encryptée.

6. Méthode selon les revendications 1 à 5, caractérisée en ce que la clé d'appariement est générée par l'unité d'utilisateur ou le module de sécurité, ou par les deux.

7. Méthode selon l'une des revendications précédentes caractérisé en ce que l'unité utilisateur est un téléphone portable et le module de sécurité est une carte SIM.

INTERNATIONAL SEARCH REPORT

national Application No

PCT/IB 01/02603

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 036 461 A (J.C. ELLIOTT) 30 July 1991 (1991-07-30) abstract; claim; figures column 7, line 5 -column 8, line 13 column 11, line 3 -column 12, line 7 -----	1-5
A	EP 0 707 290 A (CP8 TRANSAC) 17 April 1996 (1996-04-17) abstract; claims; figure 1 column 5, line 42 -column 7, line 4 -----	1,3,5
A	EP 0 530 601 A (GRUNDIG E.M.V.) 10 March 1993 (1993-03-10) -----	
A	WO 93 07715 A (THOMSON CONSUMER ELECTRONICS) 15 April 1993 (1993-04-15) -----	
A	WO 99 01848 A (SONERA OY) 14 January 1999 (1999-01-14) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

national Application No

PCT/IB 01/02603

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0997853	A	03-05-2000	DE 19850308 A1 EP 0997853 A1	11-05-2000 03-05-2000
WO 9925140	A	20-05-1999	WO 9925140 A1 AT 205990 T AU 4769797 A DE 59704698 D1 EP 1029421 A1	20-05-1999 15-10-2001 31-05-1999 25-10-2001 23-08-2000
EP 0448369	A	25-09-1991	FI 901450 A AT 159134 T DE 69127845 D1 DE 69127845 T2 EP 0448369 A2 JP 7074856 A US 5266782 A	23-09-1991 15-10-1997 13-11-1997 26-02-1998 25-09-1991 17-03-1995 30-11-1993
EP 0663650	A	19-07-1995	DE 4342641 A1 EP 0663650 A2	22-06-1995 19-07-1995
US 5036461	A	30-07-1991	NONE	
EP 0707290	A	17-04-1996	FR 2725537 A1 AU 690324 B2 AU 3318795 A BR 9504355 A CA 2160223 A1 EP 0707290 A1 JP 8212066 A KR 214817 B1 NO 954028 A US 5825875 A	12-04-1996 23-04-1998 16-05-1996 08-10-1996 12-04-1996 17-04-1996 20-08-1996 02-08-1999 12-04-1996 20-10-1998
EP 0530601	A	10-03-1993	DE 4129067 A1 AT 152538 T DE 59208418 D1 EP 0530601 A2	04-03-1993 15-05-1997 05-06-1997 10-03-1993
WO 9307715	A	15-04-1993	AU 2574092 A DE 69228481 D1 DE 69228481 T2 WO 9307715 A1 EP 0606287 A1 ES 2129043 T3 US 5835864 A	03-05-1993 01-04-1999 12-08-1999 15-04-1993 20-07-1994 01-06-1999 10-11-1998
WO 9901848	A	14-01-1999	FI 972840 A AU 739707 B2 AU 7770798 A EP 0993662 A1 WO 9901848 A1 JP 2002511964 T NZ 502166 A	03-01-1999 18-10-2001 25-01-1999 19-04-2000 14-01-1999 16-04-2002 29-06-2001

INTERNATIONAL SEARCH REPORTRAPPORT DE

pande internationale No
PCT/IB 01/02603A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 997 853 A (DETEMOBIL) 3 mai 2000 (2000-05-03)	1-3,7
A	le document en entier	6
Y	WO 99 25140 A (SWISSCOM) 20 mai 1999 (1999-05-20)	1-3,7
A	abrégé; revendications; figures	5
Y	EP 0 448 369 A (NOKIA MOBILE PHONES) 25 septembre 1991 (1991-09-25)	1-4
A	le document en entier	7
Y	EP 0 663 650 A (SIEMENS) 19 juillet 1995 (1995-07-19)	1-4
	le document en entier	
	-/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

29 mai 2002

Date d'expédition du présent rapport de recherche internationale

05/06/2002

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Fonctionnaire autorisé

David, J

INTERNATIONAL SEARCH REPORTRAPPORT DE

mande Internationale No

PCT/IB 01/02603

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 036 461 A (J.C. ELLIOTT) 30 juillet 1991 (1991-07-30) abrégé; revendication; figures colonne 7, ligne 5 -colonne 8, ligne 13 colonne 11, ligne 3 -colonne 12, ligne 7 —	1-5
A	EP 0 707 290 A (CP8 TRANSAC) 17 avril 1996 (1996-04-17) abrégé; revendications; figure 1 colonne 5, ligne 42 -colonne 7, ligne 4 —	1,3,5
A	EP 0 530 601 A (GRUNDIG E.M.V.) 10 mars 1993 (1993-03-10) —	
A	WO 93 07715 A (THOMSON CONSUMER ELECTRONICS) 15 avril 1993 (1993-04-15) —	
A	WO 99 01848 A (SONERA OY) 14 janvier 1999 (1999-01-14) —	

INTERNATIONAL SEARCH REPORT RAPPORT DE

Renseignements relatifs aux membres de familles de brevets

pande internationale No

PCT/IB 01/02603

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0997853	A	03-05-2000	DE 19850308 A1 EP 0997853 A1	11-05-2000 03-05-2000
WO 9925140	A	20-05-1999	WO 9925140 A1 AT 205990 T AU 4769797 A DE 59704698 D1 EP 1029421 A1	20-05-1999 15-10-2001 31-05-1999 25-10-2001 23-08-2000
EP 0448369	A	25-09-1991	FI 901450 A AT 159134 T DE 69127845 D1 DE 69127845 T2 EP 0448369 A2 JP 7074856 A US 5266782 A	23-09-1991 15-10-1997 13-11-1997 26-02-1998 25-09-1991 17-03-1995 30-11-1993
EP 0663650	A	19-07-1995	DE 4342641 A1 EP 0663650 A2	22-06-1995 19-07-1995
US 5036461	A	30-07-1991	AUCUN	
EP 0707290	A	17-04-1996	FR 2725537 A1 AU 690324 B2 AU 3318795 A BR 9504355 A CA 2160223 A1 EP 0707290 A1 JP 8212066 A KR 214817 B1 NO 954028 A US 5825875 A	12-04-1996 23-04-1998 16-05-1996 08-10-1996 12-04-1996 17-04-1996 20-08-1996 02-08-1999 12-04-1996 20-10-1998
EP 0530601	A	10-03-1993	DE 4129067 A1 AT 152538 T DE 59208418 D1 EP 0530601 A2	04-03-1993 15-05-1997 05-06-1997 10-03-1993
WO 9307715	A	15-04-1993	AU 2574092 A DE 69228481 D1 DE 69228481 T2 WO 9307715 A1 EP 0606287 A1 ES 2129043 T3 US 5835864 A	03-05-1993 01-04-1999 12-08-1999 15-04-1993 20-07-1994 01-06-1999 10-11-1998
WO 9901848	A	14-01-1999	FI 972840 A AU 739707 B2 AU 7770798 A EP 0993662 A1 WO 9901848 A1 JP 2002511964 T NZ 502166 A	03-01-1999 18-10-2001 25-01-1999 19-04-2000 14-01-1999 16-04-2002 29-06-2001

THIS PAGE BLANK (USPTO.)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)